Avocado

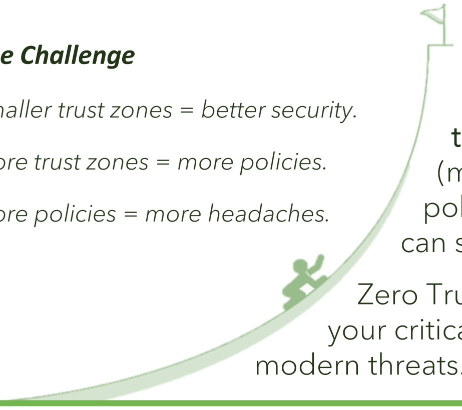
Comprehensive Zero Trust:
Automated Everywhere.

Automated Zero Trust for Workloads

Perimeter security is a necessary front-line defense for any data center. In today's complex and agile security landscape, perimeters have become porous due to complex attacks that abuse cloud misconfigurations, stolen credentials, remote code injections, and more.

Many major companies are shifting to a "Zero Trust Architecture" (ZTA) by applying the principle of least privilege to people, data, devices, and workloads. Applications and databases are often the most critical piece of any modern data center, but they're also the most difficult to zero-trust.

NIST SP 800-207 establishes the grouping and zero-trusting of applications as the gold standard. However, getting there can be quite a challenge.



The Challenge

Smaller trust zones = better security.

More trust zones = more policies.

More policies = more headaches.

Companies need to **discover** all their assets (difficult for API's and complicated apps), then **create** and **test** policies for every application group (micro-segment). Finally, they **deploy** the policies across their ecosystems, which can slow or compromise app functionality.

Zero Trust for Workloads is necessary to secure your critical applications and workloads against modern threats. How can we make it feasible?

Complete Zero Trust, without the headaches.

ZTA initiatives slowing you down? Worried about the inherent complexity?
We've got you covered.

Peace of mind.

- Eliminate threats inside your perimeter with AI & ML
- Remediate easily with powerful visualization & reporting tools
- Dynamic, auto-created policies react in real-time

Save time and money.

- Discover & map your ecosystem in hours instead of weeks
- Costs 70% less than typical east-west hardware

Avocado: Automating ZTA Everywhere.

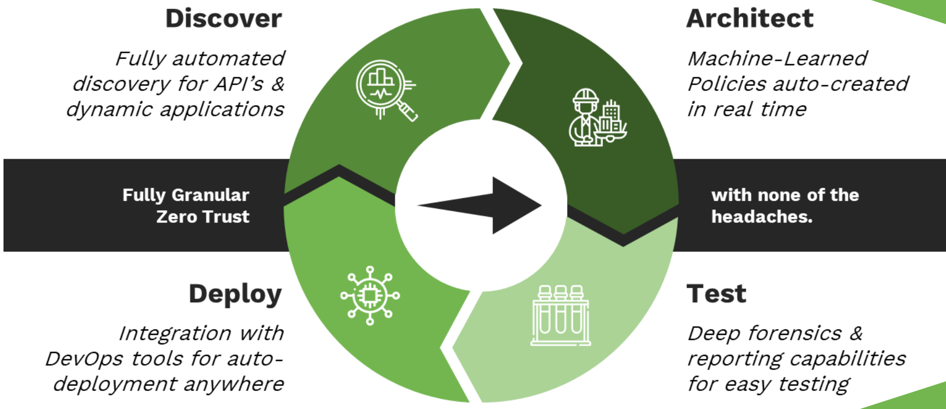
Perimeter security is a necessary front-line defense for any data center. In today's complex and agile security landscape, perimeters have become porous due to complex attacks that abuse cloud misconfigurations, stolen credentials, remote code injections, and more.

Advanced Auto-Discovery

- Skip countless meetings with devs & architects
- Discover & unpack apps to their process level
- Find dynamic apps, API's, etc. in any environment

Process-Native Segmentation

- Industry-leading performance
- Segment from the ground-up
- No manual policies or maintenance
- Most granular solution available



Discover

Fully automated discovery for API's & dynamic applications

Architect

Machine-Learned Policies auto-created in real time

Fully Granular Zero Trust

with none of the headaches.

Deploy

Integration with DevOps tools for auto-deployment anywhere

Test

Deep forensics & reporting capabilities for easy testing

For inquiries, contact info@avocadosys.com or visit us at www.avocadosys.com